Study of Single Family Property Management Systems and Data

RISK ANALYSIS

June 16, 2003

Office of Housing

Federal Housing Administration

Department of Housing and Urban Development

Risk Analysis

Table of Contents

Page #

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

The Federal Housing Administration's (FHA's) Office of Insured Single Family Housing administers a property management program and oversees the acquisition, marketing, and disposition of approximately 60,000 properties per year. Single Family Housing maintains the Single Family Acquired Asset Management System (SAMS) and other property management support systems to assist with program operations, such as case management, financial management, contractor monitoring, business evaluation, and business partner management. SAMS and the other systems must fully support these business functions in order for FHA to effectively and efficiently manage its program.

Since the original implementation of SAMS, Single Family Housing has changed the property management program and its business model. In an effort to streamline operations, FHA began contracting out the Real Estate Owned (REO) functions in 1997. Consequently, Single Family Housing's role shifted to oversight and monitoring rather than performing the day-to-day REO activities. Over time, FHA adapted SAMS and developed supplemental systems to support both the property management and contractor oversight functions. While FHA has made extensive modifications to SAMS and developed other support systems, numerous challenges remain with its property management operations within the current systems environment. For example, maintenance costs remain excessively high. Furthermore, FHA has received criticisms from the General Accounting Office (GAO) about its single-family property management operations, systems, and monitoring performance in various studies. As a result, GAO has placed Single Family on its high-risk list since 1994. In its financial statements, FHA also has received material weaknesses and reportable conditions related to single-family systems, including:

- FHA's systems environment provides insufficient support to its business processes.
- FHA lacks control over budget execution and funds.
- FHA performs inadequate monitoring over its Single Family property inventory.

1.1 Purpose

Single Family Housing seeks to increase SAMS' functionality or implement a new system. FHA needs to assess its long-term business needs and the capacity of its current systems prior to any further systems development efforts. The *Risk Analysis* provides an approach for conducting risk assessments of the proposed property management solution. FHA identifies the project management structure, the risk management structure, and its schedule for periodic risk assessments. In this document, FHA:

- Begins system security planning.
- Analyzes and identifies the security threats and potential vulnerabilities of the proposed system.
- Determines the necessary measures to be taken to safeguard the system.
- Evaluates the identified measures for cost and economic feasibility.

1.2 Scope

This project provides FHA with a blueprint for property management and helps guide FHA towards an improved way of conducting its business. FHA performed an in-depth review of the

Single Family systems supporting the property management function, including asset management, business participant management, business evaluation, and financial management. Based on this analysis, we presented an alternative solution to its current systems environment. FHA conducted this study in five primary phases:

- Phase I – Identify major business and system needs.
- Phase II – Identify major deficiencies in the current systems.
- Phase III – Develop short- and long-term alternatives.
- Phase IV – Present findings and obtain stakeholder buy-in.
- Phase V – Develop Initiate phase documents, including the *Project Plan, Needs Assessment, Feasibility Study, Risk Analysis, Cost-Benefit Analysis, System Security Plan,* and *Systems Decision Paper*.

1.3 System Overview

While the Department of Housing and Urban Development's (HUD) Information Technology (IT) division provides technical assistance, HUD's Office of Housing is responsible for the identification of business process and reporting needs of its systems. For single-family mortgage insurance programs, the Office of Single Family Programs and the Office of the Comptroller share responsibility for SAMS and other single-family systems.

SAMS is a mixed program and financial management system that accounts for the sale of over 60,000 properties per year valued at over $5 billion dollars with related expenses totaling nearly $1 billion. SAMS supports HUD staff at Headquarters, Homeownership Centers (HOCs), and Management and Marketing (M&M) contractors with tracking single-family properties from acquisition through resale. In addition to collecting data related to the management, marketing, and disposition of properties, SAMS maintains financial records in compliance with the Federal Credit Reform Act and processes disbursements to M&M contractors, vendors, taxing authorities, and homeowners' associations.

SAMS is hosted on HUD's IBM-compatible mainframe and is connected to HUD's network, HINET, through a COMTEN front-end processor. Software used in SAMS includes: COBOL, DB2, CICS, EXTRA, JCL, NOMAD, and the Configuration Management tool, Endevor. SAMS development tools include Electronic Data System's (EDS) proprietary case tool – INCASE.

The following table provides the requisite system information.

Responsible Organization	Federal Housing Administration – Office of Housing
System Name or Title	Single Family Acquired Asset Management System
System Code	A80S
Project Cost Accounting Sub-system (PCAS) Number	To Be Determined
System Category	Major application
Operational Status	Operational

Users	FHA and M&M contractors
System Input	Mortgagee data, transmittal check data, property acquisition data, claim data, lockbox and Fedwire collection data, check data, valid property case data, property maintenance data, property acquisitions
System Output	New acquisitions, inventory status and sales data, property listing, property title data, SAMS general ledger balances, disbursement data, and sales related data.
Interaction With Other Systems	The SAMS environment is composed of numerous interconnected and stand alone systems. SAMS shares data with the following systems through manual or automated interfaces: Single Family Insurance System (SFIS), Computerized Homes Underwriting Management System (CHUMS), Institutional Master File (IMF), A80N, Single Family Insurance Claims Subsystem, Lockbox, File Transfer Protocol (FTP) Server, HUD Web, Kiosks, Single Family Data Warehouse, TEAM, Fedwire system (Cashlink), Cash Control Accounting Reporting System (CCARS), ECS system (Electronic Funds Transfer (EFT) disbursements), and the FHA Subsidiary Ledger

1.4 Project References

FHA used the following reference materials to prepare the *Risk Analysis*.

Document	Date
EDS, HUD/SAMS Release Summary	No date noted
Information Technology Reform Act of 1996	No date noted
IBM Endowment for the Business of Government, *IT Outsourcing: A Primer for Public Managers*, Chen, Perry	February 2003
Joint Financial Management Improvement Program, *Property Management System Requirements*	October 2002
Management & Marketing Service Contract Terms and Conditions	No date noted
National Institute of Standards and Technology*, Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook*	October 1995
National Institute of Standards and Technology, *Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems*	September 1996

Document	Date
National Institute of Standards and Technology, *Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model*	April 1998
National Institute of Standards and Technology, *Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems*	December 1998
National Institute of Standards and Technology, *Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems*	November 2001
National Institute of Standards and Technology, *Special Publication 800-40, Procedures for Handling Security Patches*	August 2002
National Institute of Standards and Technology, *Special Publication 800-44, Guidelines on Securing Public Web Servers*	September 2002
Office of Management and Budget Circular Number A-130, *Management of Federal Information Resources, Appendix III*	November 2000
United States Department of Housing and Urban Development, *Business Process Reengineering*	March 1997
United States Department of Housing and Urban Development, *FHA Audit of Financial Statements Fiscal Years 2002 and 2001*	January 2003
United States Department of Housing and Urban Development, *Final Draft SAMS User's Guide*	August 2002
United States Department of Housing and Urban Development, *Management Structure Design and Specifications in the M&M Contract Environment For Single Family Property Disposition*	January 1999
United States Department of Housing and Urban Development, *M&M Contractor Compliance Review, Risk-Based Targeting Model Web Tool Training*	August 2002
United States Department of Housing and Urban Development, *Office of the Single Family Housing Target Architecture Development*	September 2002
United States Department of Housing and Urban Development, *Processing Procedures and Internal Controls for M&M Contractors*	No date noted
United States Department of Housing and Urban Development, *SAMS Reports Training Manual*	May 2002

Document	Date
United States Department of Housing and Urban Development, *Single Family Housing Target Architecture*	August 2002
United States General Accounting Office, *Financial Management: Strategies to Address Improper Payments at HUD, Education, and Other Federal Agencies*	October 2002
United States General Accounting Office, *Information Technology: Leading Commercial Practices for Outsourcing of Services*	November 2001
United States General Accounting Office, Loan Origination and Foreclosed Property Management Processes	November 1999
United States General Accounting Office, *Single Family Housing: Current Information Systems Do Not Fully Support the Business Processes at HUD's Homeownership Centers*	October 2001
United States General Accounting Office, *Single Family Housing: Improvements Needed in HUD's Oversight of the Property Sale Process*	April 2002
United States General Accounting Office, *Single Family Housing: Stronger Measures Needed to Encourage Better Performance by Management and Marketing Contractors*	May 2002

1.5 Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in this document.

Acronym/Abbreviation	Definition
ADP	Automatic Data Processing
ASP	Application Service Provider
CCARS	Cash Control Accounting Reporting System
CHUMS	Computerized Homes Underwriting System
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CO	Contracting Officer
COBIT	Control Objectives for Information and related Technology
EDS	Electronic Data Systems

Acronym/Abbreviation	Definition
EFT	Electronic Funds Transfer
FHA	Federal Housing Administration
FISCAM	Federal Information Systems Controls Audit Manual
FTP	File Transfer Protocol
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GTM	Government Technical Monitor
GTR	Government Technical Representative
HOC	Homeownership Center
HUD	U.S. Department of Housing and Urban Development
IMF	Institutional Master File
ISACA	Information System’s Audit and Control Association
IT	Information Technology
M&M	Management and Marketing
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCPO	Office of the Chief Procurement Officer
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PCAS	Project Cost Accounting Sub-System
QA	Quality Assurance
REO	Real Estate Owned

Acronym/Abbreviation	Definition
SAMS	Single Family Acquired Asset Management System
SDM	System Development Methodology
SFIS	Single Family Insurance System

1.6 Point of Contact

The following sections provide a listing of contacts for additional information regarding this document and the overall project, as well as a listing of departmental organizations and their contacts that provide support and guidance related to this project.

Type of Contact	Contact Name	Department	Telephone	Email/Address

1.6.1 Information

This table provides a list of organizational points of contact that may be needed by the document user for informational and troubleshooting purposes. All contacts are located at 451 Seventh Street, SW, Washington, DC, 20410.

Type of Contact	Contact Name	Department	Telephone	Email/Address

1.6.2 Coordination

The following table provides a list of organizations that require coordination between the project and its specific support function.

Type of Contact	Contact Name	Department	Telephone	Email/Address

2.0 PROJECT AND SYSTEM DESCRIPTION

2.0 PROJECT AND SYSTEM DESCRIPTION

Risk and issue management is important to any project's success. Project management requires the planning of milestones and activities as well as the identification and allocation of resources to carry them out. The *Risk Analysis* provides an approach for conducting risk assessments for the implementation of the proposed property management system and also assesses the overall security posture of the technical environment for the proposed property management system.

Risk management is made up of two primary activities: risk assessment and risk mitigation. These activities encompass the defining of boundaries for review, the collection and analysis of data, and the interpretation of risk analysis results. The process also entails the selection and implementation of security controls and safeguards to reduce risk to a level acceptable to management within applicable constraints.

2.1 Summary

FHA performed an in-depth study of Single Family systems supporting the property disposition program. The objective of this study was to determine the best option for FHA's property management systems, particularly SAMS and the related support systems. Based on FHA's findings from the Initiate phase of this project, FHA concluded that the best option is to replace SAMS with a modern, web-based property management system hosted outside of the HUD technical environment by an industry-proven Application Solution Provider (ASP). As part of this option, the FHA subsidiary ledger will process financial management functions, including accounting and funds control, for the property management system. Program staff will work with the FHA subsidiary ledger project team to build a rule-based interface that will facilitate the exchange of information between the new property management system and the FHA subsidiary ledger.

This risk analysis is being completed for the proposed property management system. For the proposed solution, an ASP will host the web-based property management application on its own servers within its own facilities. It is expected that the ASP will also provide full-lifecycle services for implementation as well as training and ongoing operational support. The service provider will shoulder the burden of database and programming administration, application security, backup processing, and core hardware acquisition, support, and maintenance.

2.1.1 Project Management Structure

The integrated project team will include the project director, project leader, several technical and business experts from the Program Area, contractors from the ASP, and several other contractors to handle different areas of the project, such as business process redesign and change management. The team will work to:

- Define needs and requirements.
- Verify that these requirements are implemented correctly.
- Direct the project through the lifecycle.
- Provide the technical lead and broad technical direction expertise.
- Develop project plans and schedules.

- Ensure the project stays on budget and schedule.

Joe McCloskey, Director of Single Family Asset Management Division, and Ron Crupi, Director of Single Family Accounting are the project co-sponsors. FHA will document expected start and end dates for system implementation in the project workplan. The workplan is incorporated as part of the *Project Plan*.

2.1.2 Project Staffing

FHA expects to have a project team comprised of several smaller project area teams. The project area teams, as well as detailed roles, responsibilities, and representative work products for the project area team members are presented in Appendix A. FHA will determine the number of resources required per project area team as the project progresses.

2.2 Risk Management Structure

FHA will work with OCFO, OCIO, and OIT to manage identified risks and maintain countermeasures. Throughout the duration of the project, FHA will review the risks and safeguards to ensure that the project team mitigates the known risks and identifies any new risks and safeguards, as necessary.

The risk assessment determines what the vulnerabilities are, determines the likelihood that threats will exploit a given vulnerability, and predicts the potential impact to the system if the vulnerability is exploited. The project team seeks to anticipate problems and pre-plan, wherever possible, ways to reduce their probability of occurrence and to mitigate their impact should they occur. The early identification of risks and the swift resolution of issues enable project management to be proactive in their decision making and management. The project team, in conjunction with OCFO, OCIO, and OIT, will:

- Identify potential obstacles and risks.
- Assess the impact of risks.
- Assign a priority to potential risks.
- Develop corrective actions should the risk occur.
- Develop a strategy to resolve issues.
- Monitor the issues and risk to closure.

2.3 Periodic Risk Assessment

In conjunction with the ASP, FHA will perform a comprehensive risk assessment to evaluate the soundness of its computer security program's ability to protect the department's assets and compliance with federal directives. The assessment will address many issues at the programmatic and system level.

The team assigned to perform periodic risk assessments will analyze the severity of the documented risks and note any changes that have occurred since the last assessment. Periodic assessments, scheduled to occur every three to six months during the development of the system, will provide an opportunity to document new system risks that have arisen and that may impact the future health of the system. Risks can be identified at any time during the project's lifecycle. Once the system is in production, FHA will conduct periodic risk assessments when significant changes occur.

Through periodic risk assessments, the team will incorporate any issues or problems identified in the normal course of business into the *Risk Analysis* throughout the system development lifecycle. The project leads and area managers will discuss the status of open issues and risks during management meetings and document the issues for tracking purposes. The team will revisit the identified risks during future risk analysis processes.

2.4 Contingency Planning

Contingency planning addresses how to keep an organization's critical functions operating in the event of disruptions, large or small. FHA will work with the ASP to develop a comprehensive contingency plan once the contract is awarded. For the new system, FHA will work with the ASP to:

- Identify the most critical and sensitive operations and their supporting computer and personnel resources.
- Define recovery requirements and timeframes to ensure a balance between cost effectiveness and risk mitigation.
- Develop and document a comprehensive contingency plan.
- Test the contingency/disaster recovery plan.

3.0 SYSTEM SECURITY

3.0 SYSTEM SECURITY

The objective of system security planning is to improve protection of information technology (IT) resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan.

Security requirements, expressed as technical features (e.g., access controls), assurances (e.g., background checks for system developers and users), operational practices (e.g., awareness and training) come from a number of sources including law, policy, applicable standards and guidelines, functional needs of the system, and cost-benefit trade offs.

FHA has developed the *System Security and Privacy Plan* in accordance with Office of Management and Budget (OMB) *Circular A-130, Management of Federal Information Resources* and the HUD System Development Methodology (SDM). The *System Security and Privacy Plan* provides an overview of the security requirements of the proposed property management system and addresses information sensitivity, levels of security, security risks, technical features, assurances, and operational practices.

Given the importance of the proposed system to FHA's mission, FHA has developed the *System Security and Privacy Plan* during the Initiate phase – rather than Define phase – of the SDM. The security plan was developed during the Initiate phase to begin system security planning early in the system development lifecycle. However, the plan is only an initial draft and will need to be revised to reflect updated security requirements during subsequent project phases.

3.1 Baseline Security Requirements

This document uses the baseline security requirements to perform the risk assessment. The baseline security requirements are derived from Federal law, HUD requirements, and other government directives. FHA analyzed these requirements to assess the risks of this project and to determine the extent to which these risks may directly impact the security posture of the system.

This table identifies baseline security activities and the proposed frequency with which to conduct these baseline security activities. These activities correspond with *OMB Circular A-130, HUD SDM, Government Information Security Reform Act (GISRA), GAO's Federal Information Systems Controls Audit Manual (FISCAM),* and Information System's Audit and Control Association's (ISACA) *Control Objectives for Information and related Technology (COBIT)* requirements for major application systems.

Activity	Frequency
Establish Security Point of Contact	Ongoing.
Prepare *System Security and Privacy Plan* and related SDM documents	Complete the *System Security and Privacy Plan* during the Initiate and Define Phases. Incorporate security updates, results of reviews, and summary of actions taken during subsequent phases (published as part of the *System Decision Paper* revisions) on an on-going basis.
Gather Security Requirements	Complete the System Requirements for new systems and system upgrades during the Development phase.
Perform Review of Controls	For new systems, perform review of controls prior to the design approval. For existing systems, update controls every three years as a minimum.
System Security Plan Authorization	Update System Security Plan on a yearly basis after initial plan is complete, including Authorization.
Business Resumption Plan (Headquarters) – Contingency Plan	Update plan every year as a minimum. Any changes should be incorporated as soon as possible.
OMB A-130 Review - all sites and support systems	Annual.
Maintain Access Controls (Security Software)	Ongoing.

FHA will assess security requirements and specifications necessary to safeguard the system and its corresponding data based on the environment, scope, sensitivity of the data, and criticality of the proposed system. These security controls will ensure that FHA adequately counteracts security risks that threaten the proposed property management system and implements safeguards to protect the system and its corresponding data.

Section 3.0 of the *System Security and Privacy Plan* addresses the system security risks and corresponding control measures in greater detail.

3.2 Baseline Security Safeguards

FHA needs to protect its assets against errors and potential loss of data and interruption of operations. HUD's Critical Infrastructure Protection (CIP) program provides a framework and scheduled activities to manage risk, develop security policies, assign responsibilities, and monitor the adequacy of the ongoing implementation of HUD's physical and information system security controls. The CIP program includes a methodology to assess security risk, develop and implement effective security procedures, conduct security awareness and training, develop disaster recovery and contingency plans, and to monitor the effectiveness of these procedures. The FHA project team will follow the CIP program to define the detailed security requirements and safeguards.

Section 3.0 of the *System Security and Privacy Plan* addresses the system security risks and corresponding control measures in greater detail.

3.3 Sensitivity Level of Data

The sensitivity and criticality of the information stored within, processed by, or transmitted by a system will provide a basis for the value of the system and is one of the major factors in risk management.

FHA's Office of Insured Single Family Housing administers the property management program and oversees the acquisition, marketing, and disposition of approximately 60,000 properties per year. The proposed property management system will assist with program operations, such as asset management, financial management, business evaluation, and business partner management. As a result, the proposed property management system will contain confidential information, such as buyer social security numbers. It will also store property appraisal, bid, sales, and other financial information. Furthermore, financial information will be collected and transferred through a rules-based engine to FHA's subsidiary ledger for financial management, recordation, and funds control.

The need for HUD-established security policies are critical to realizing Single Family's mission, including physical security, non-disclosures, background checks, intrusion detection, counterfraud, anti-virus, and installation of firewalls. To comply with *OMB Circular A-127*, *Policies and Standards for Financial Management Systems*, FHA needs to identify security controls and incorporate these controls into operations in accordance with the *Computer Security Act* and *OMB Circular A-130, Management of Federal Information Resources, Appendix III.* For those financial systems that contain sensitive information, agencies must implement and maintain a security program to assure adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in major applications.

Section 2.0 of the *System Security and Privacy Plan* addresses the sensitivity of the data contained in the proposed system in greater detail.

3.4 User Security Investigation Level and Access Need

Effective administration of users' computer access is essential to maintain system security. User account management focuses on identification, authentication, and access authorizations. These controls are augmented by the process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations.

Identification and authentication is a technical measure that prevents unauthorized people from entering an IT system. The new property management system will have access controls that will identify, differentiate, and authenticate users via passwords, tokens, or other devices. The preferred method of authentication requires the use of digital certificates that provide the element of technical non-repudiation. Use of digital certificates and mutual authentication (client to server, server to client) assures users are properly authenticated and their identity is clearly established. The system will also use role-based access controls to enforce segregation of duties and to restrict users to authorized transactions and functions.

FHA will develop an application role user matrix to define user identification, correlation of actions to users, maintenance of user ids and user lists, identification and authentication, and logical access controls. The matrix will define users with direct access to the system and those who will indirectly receive output from the system. The matrix will also include the levels of security investigation and system access required for each user. FHA will work with the ASP to ensure the property management system maintains accurate access levels for each user.

Other security requirements may include:

- Prohibiting access scripts with embedded passwords.
- Limiting invalid access attempts for a given user.
- Implementing procedures for handling lost and compromised passwords.

4.0 RISKS AND SAFEGUARDS

4.0 RISKS AND SAFEGUARDS

HUD identifies and addresses system risks in two SDM documents – the *System Security and Privacy Plan* and the *Risk Analysis.* The *System Security and Privacy Plan* presents management, operational, and technical risks. Alternatively, the *Risk Analysis* focuses on the following risk areas:

- Physical risks – Risks associated with vulnerability of facilities and the computer room and the impact of environmental hazards on the computer, related equipment, and their contents.
- Management risks – Risks associated with project management tasks and control over the application, database, and network.
- Software risks – Risks associated with potential vulnerabilities of software products, such as applications or middleware.

Different assets of FHA are subject to different kinds of threats. Some are considered less likely than others, and the potential impact of different threats may vary greatly. The preparer and reviewer of risk assessments estimate the likelihood of these threats. A good security program relies on an integrated, cost-effective collection of physical, procedural, and automated controls to prevent threats from harming assets.

The remainder of this section categorizes, assesses the impact, and summarizes the safeguards for each risk identified during the Initiate phase of this project. This section will be updated during each subsequent phase of the project.

4.1 Control Risk

In the proposed future environment, an ASP will host the property management application on its own servers within its own facilities. The ASP not only hosts the application, but will provide full-lifecycle services for implementation as well as training and ongoing operational support. The service provider will shoulder the burden of database and programming administration, application security, backup processing, and core hardware acquisition, support, and maintenance.

Although there are numerous benefits to be gained by outsourcing these services, FHA may experience some loss of direct management control over the property management system. Loss of direct management control over project scope, technologies, costs, and IT direction are some factors of control risk.

Managing and monitoring an outsourced contract can be a time-consuming and a resource-intensive project. Tasks include system transition and implementation, performance evaluation, and service adjustments. Additionally, HUD will need to shift its focus from procurement to service and relationship management. Lack of monitoring could result in major system disruptions, such as system downtime, data integrity concerns, and delays in processing system interfaces. Additionally, poor communication and lack of joint problem-solving mechanisms may cause missed opportunities for early problem detection and continuous improvement.

4.1.1 Risk Category and Business Impact

This is a management risk. Lack of proper controls over contractor performance could lead to loss of control over the system and program.

4.1.2 Potential Safeguards

Potential safeguards to mitigate contract risk include:

- **Form a partnership with the vendor –** In developing a partnership, the project management team should focus on creating a strong working relationship with the ASP and promoting frequent, open communication throughout the project lifecycle. A partnership helps align incentives and in the long run, create win-win solutions for both parties. Open communication must exist for both parties to reap the most benefit from the partnership. For instance, HUD needs to rely on the vendor to be forthcoming about potential problems or better solutions, and a strong partnership will help foster this type of environment.[1]
- **Develop a well-written contract –** A well-written contract with detailed service level agreements is essential for mitigating control risks and is the foundation for developing a strong working relationship with the ASP. The contract should be written in a fashion that fosters a strong partnership with the vendor while protecting HUD's interests. There are several key factors for developing an effective contract. FHA should research and utilize best practices and lessons learned in the area of contract negotiation for procurement of IT services before finalizing any contract with an ASP. FHA should research examples set by other organizations that elected to use an ASP and analyze lessons learned from similar IT projects both internal and external to HUD. FHA should structure the contract to protect FHA in the event the ASP cannot meet the terms of the contract or other foreseeable scenarios. FHA should take the necessary precautions to maintain rights to the application and data in the event the vendor cannot meet its contractual obligations. FHA should use service level agreements to ensure that the selected vendor fulfills requirements specified during contract negotiation. Service level agreements should be structured to closely align with HUD's performance-based contract initiative to give HUD the ability to withhold payments based on poor performance, and should have provisions for benchmarking, technological change, and termination. FHA should consider procuring the help of a third-party that specializes in contract negotiations for similar IT services contracts.

4.2 Security Risk

Security risk includes threats to communication, the property management system database and application, and the vendor's facilities. For the proposed solution, the application and database are stored outside of the HUD technical environment at the vendor's facilities. HUD systems communicate with the ASP via a network. As such, the network-connected systems between HUD and the ASP are exposed to security threats.

If the vendor's main technology infrastructure is shared by multiple client organizations, there can be multiple sources of security threats. Other client organizations have authorized access to the vendor's site and may be sharing the application and database servers. As such, there is

[1] Chen, Yu-Che; Perry, James. IT Outsourcing: A Primer for Public Managers. February 2003.

the increased security threat of other organizations accessing FHA data as it resides within the vendor's facilities.[2]

In addition, the hardware that supports the application resides at the vendor's facility. The vendor is responsible and will be measured for taking precautions to protect the hardware from environmental and personnel hazards.

4.2.1 Risk Category and Business Impact

This is software and physical risk. The software risk is associated with breaches of security when unauthorized users access the property management systems database or application. Physical risk is associated with disruptions of service due to hardware malfunctions.

4.2.2 Potential Safeguards

Potential safeguards to mitigate security risk include:

- **Research the viability of dedicated application and database servers** – Price permitting, FHA should request dedicated application and database servers during contract negotiations. In addition to security concerns, performance may be slowed when sharing database and application servers. As part of the vendor site visit, HUD should explore system load testing to review system performance and make system performance a key aspect of the service level agreement.
- **Address security requirements established in this document and the *System Security and Privacy Plan*** – FHA should implement system security features defined in Section 3 of this document. In addition, FHA also has developed the *System Security and Privacy Plan* to identify the security requirements for the new property management system. The security plan defines such areas as identification and authentication, logical and physical access to the system and its resources, communication, and hardware and software issues. The *System Security and Privacy Plan* will be revised to reflect future security considerations during subsequent project phases.
- **Review the vendor's facilities and business continuity plan** – FHA should research the vendor's security capabilities. Conducting on-site visits provides an opportunity for FHA to assess the reliability of the vendor's facilities and security. Business continuity should be a priority and adhere to the guidelines that HUD has developed for internal systems. The plan should address the vendor's preparedness for disruptions in service and for changing operational priorities. Business continuity can be measured in uptime – the percentage of time that the system is available to HUD and its M&M contractors. HUD should look for a vendor who can provide uninterrupted service by either the creation of redundant service units or by immediate backup and restore services.
- **Address personnel training and background screening of the vendor's IT personnel** – User training occurs during and after implementation. Training should include correct methods to access the system and a discussion regarding security concerns. The IT personnel at the vendor's site should be qualified and possess experience in supporting HUD's system needs. In addition to standard references, background checks on the

[2] Chen, Yu-Che; Perry, James. IT Outsourcing: A Primer for Public Managers. February 2003.

vendor's IT personnel should be performed. The contract should also address changes in IT personnel who support HUD's property management account.

4.3 Vendor Risk

The viability and stability of the vendor is a major concern. A competitive marketplace may have a significant impact on the vendor's viability. As such, there have been instances where vendors have gone out of business without any clear warning signs. Additionally, there has been a history of mergers and acquisitions in the software industry.

4.3.1 Risk Category and Business Impact

This is a software and management risk. In the ASP solution, the vendor is providing the property disposition software and the hardware that hosts the software. If the vendor should fail, HUD may lose the ability to use the system and lose access to the data stored in the database without proper precautions in place.

4.3.2 Potential Safeguards

Potential safeguards include:

- **Research and select a mature vendor with extensive industry experience and a solid financial position** – FHA should carefully scrutinize the potential vendors for established market leaders. FHA should analyze the history and financial position of potential vendors. Conducting on-site visits provides an opportunity for the vendor to demonstrate the reliability of their facilities and security. Additionally, FHA should communicate with other customers, and possibly arrange on-site visits, to obtain information on the level of customer satisfaction with the particular vendor's performance. FHA should select a vendor with a strong financial position and a proven record of providing long-term service to its customers.
- **Add terms and conditions to the contract that address mergers and acquisitions as well as possible failure of the vendor to provide the software and application services** – FHA should account for the possibility of mergers and acquisitions in the contract. Performance-based service level agreements should be included in the contract. More recommendations on drafting a comprehensive contract are detailed in section 4.1.2.

4.4 Integration Risk

FHA may face technical challenges in developing the required interfaces between the ASP solution, the FHA subsidiary ledger, and other HUD systems. At this time, FHA has not completed the implementation of all PeopleSoft modules for the subsidiary ledger, including Accounts Payable, Accounts Receivable, and Budget. In addition, with the department in the process of defining its enterprise architecture, FHA may need to complete integration efforts without established technical standards.

4.4.1 Risk Category and Business Impact

This is a software risk. In the latest audit of FHA's financial statements, the OIG sighted a material weakness for funds control. The report states, "FHA relies on manual reconciliation processes of nonintegrated systems to assess whether there is available budgetary authority prior to obligating funds. For example, to determine remaining available budgetary authority, FHA must aggregate expended amounts from certain systems including the general ledger system, SAMS, and others."[3] If FHA does not fully implement the necessary interfaces, many of the same deficiencies noted with the old system will continue to exist.

4.4.2 Potential Safeguard

- **Adhere to project management principles and the SDM** – FHA will follow HUD's SDM for the development of the interfaces and implementation of the proposed property management system. The project team will define the system and organizational requirements, prepare detailed design specifications, and develop the necessary software routines. FHA will conduct string, integration, and user acceptance testing in accordance with the SDM.
- **Acquire qualified resources to help complete tasks** – FHA will work with the ASP, several HUD offices, and other contractors to leverage the skill sets of the different organizations. FHA will create a Quality Assurance (QA) team that will work with the functional, technical, and change management teams. This QA team will review the SDM requirements and HUD policies with the project team to assure that the team complies with current standards and procedures.
- **Require new property management system to be built on an open architecture** – FHA will require the proposed property management system to be built on an open architecture. This is essential because the department is in the process of developing its enterprise architecture. An open architecture affords flexibility, scalability, and maintainability. In a networked environment, multiple platforms can be used in an open architecture. Additionally, an open architecture allows for a wider range of vendors giving FHA the best options for selecting systems based on best practices and competitive pricing. By using a system with an open architecture, it will be easier for FHA to build interfaces between the proposed property management system and other systems, such as the FHA subsidiary ledger.

4.5 Human Capital Risk

FHA may experience shortages of program and IT staff to assist with the system implementation and integration. Subject matter experts will be instrumental in detailing the business requirements to properly modify and configure the system. IT staff will support system implementation efforts as well as ongoing monitoring. Given the staffing shortages within the Asset Management and IT Divisions and the impact this risk has on the success of the project, it is crucial that FHA properly mitigate this human capital issue.

4.5.1 Risk Category and Business Impact

This is a management risk. Without the help of subject matter experts and internal IT staff to assist with this project, issues may arise while documenting functional requirements and during system implementation tasks, such as system selection, modification, configuration, and testing.

[3] United States Department of Housing and Urban Development, *FHA Audit of Financial Statements Fiscal Years 2002 and 2001*

4.5.2 Potential Safeguard

- **Hire contractors to support implementation efforts** – Due to the shortage of program and IT staff, FHA should focus on obtaining the help of contractors with knowledge of the Property Disposition program and FHA's business model to assist with the system implementation. These contractors should have experience with system implementation projects at HUD and have established relationships with HUD staff to facilitate effective communication. FHA should consider hiring a contractor to serve as a prime-integrator. Prime-integrators can assist with project management and quality assurance while providing technical assistance with areas such as security administration, data conversions, interface development, and testing.

5.0 COST AND EFFECTIVENESS OF SAFEGUARDS

5.0 COST AND EFFECTIVENESS OF SAFEGUARDS

In section 4.0, FHA identified the security threats and potential vulnerabilities of the proposed system and determined the necessary measures to safeguard the proposed system. This section evaluates the appropriate measures, and analyzes those measures for cost and economic feasibility.

5.1 Potential Safeguards – Control Risk

As defined in section 4, potential safeguards to mitigate control risk include:

- Form a partnership with the vendor.
- Develop a well-written contract.

5.1.1 Lifecycle Costs for Acceptable Safeguards

The costs of these safeguards are already included in the estimated lifecycle costs for the project and will not impose any additional costs on the project. The project will proceed under its current budget as defined in the *Project Plan*.

5.1.2 Effect of Safeguards on Risks

To mitigate control risk, FHA will develop a partnership with its selected ASP and establish clear lines of communications. FHA will also dedicate the necessary resources to develop a contract that protects its interests and promotes mutual benefits for both parties.

5.1.3 Economic Feasibility of Safeguards

By developing a partnership and establishing clear lines of communication with the ASP, FHA can reduce control risks. Failure to implement these safeguards may lead to loss of control over the system and data.

5.2 Potential Safeguards for Security Risk

As defined in section 4, potential safeguards to reduce security risk include:

- Research the viability of dedicated application and database servers.
- Address requirements established in section 3, System Security and the SDM document, *System Security and Privacy Plan.*
- Review the vendor's facilities and business continuity plan.
- Address personnel training and background screening of the vendor's IT personnel.

5.2.1 Lifecycle Costs for Acceptable Safeguards

Many of these costs are already included in the estimated lifecycle costs for the project and will not impose any additional costs on the project. Exceptions may include:

- Conducting on-site visits to assess the reliability of the vendor's facilities and security.

- Obtaining a dedicated application and database server.
- Implementing some of the security safeguards because the effectiveness of these safeguards is directly proportional to the cost.

The *Cost/Benefit Analysis* provides order-of-magnitude estimates to facilitate comparison across the various options and to supply FHA management with relative cost estimates. If FHA decides to implement these safeguards, the cost/benefit estimates will need to be adjusted.

5.2.2 Effect of Safeguards on Risks

Once a solution has been selected, FHA, in partnership with the vendor, will review all communication, application, and database storage needs. These requirements will assist in the development of a Security Plan. Additionally, FHA will follow security guidance as set forth in OMB *Circular A-130*, GISRA, GAO's *FISCAM*, National Institute of Standards and Technology (NIST) Special Publications, and ISACA's *COBIT*.

5.2.3 Economic Feasibility of Safeguards

FHA will take into account many factors before finalizing the security plan, including cost. FHA plans to implement a security plan that will mitigate security risk to an acceptable level.

5.3 Potential Safeguards for Vendor Risk

As defined in section 4, potential safeguards to reduce vendor risk include:

- Research and select a mature vendor with extensive industry experience and a solid financial position.
- Add terms and conditions to the contract that address mergers and acquisitions as well as possible failure of the vendor to provide the software and application services.

5.3.1 Lifecycle Costs for Acceptable Safeguards

The costs of these safeguards are already included in the estimated lifecycle costs for the project and will not impose any additional costs on the project, with the exception of conducting on-site visits. The project will proceed under its current budget as defined in the *Project Plan*.

5.3.2 Effect of Safeguards on Risks

During site visits, FHA would have the opportunity to meet with vendor staff that will be supporting the system, observe the system in production mode, observe the client support capabilities, and observe the results of load testing the system. When meeting with other clients, FHA would see the system in a true operational environment, would be able to meet with end-users and discuss the system capabilities, and would be able to discuss vendor's response to system support and maintenance.

5.3.3 Economic Feasibility of Safeguards

The costs associated with on-site visits to the vendor's locations are one-time, upfront costs. Detailed costs will be developed upon selection of a solution and determination of potential vendors. The tasks related to a site visit cannot be accomplished in a conference call. The benefits outweigh the associated costs.

5.4 Potential Safeguards – Integration Risk

As defined in section 4, potential safeguards to reduce integration risk include:

- Adhere to project management principles and the SDM.
- Acquire qualified resources to help complete task.
- Require new property management system to be built on an open architecture.

5.4.1 Lifecycle Costs for Acceptable Safeguards

The costs of these safeguards are already included in the estimated lifecycle costs for the project and will not impose any additional costs on the project. The project will proceed under its current budget as defined in the *Project Plan*.

5.4.2 Effect of Safeguards on Risks

By implementing the identified safeguards, FHA will reduce the risk of integration failures. A successful integration will help to eliminate long-standing audit weaknesses, such as funds control.

5.4.3 Economic Feasibility of Safeguards

It is essential that FHA complete all necessary interfaces. The interface between the property management system and the FHA subsidiary ledger will be developed in conjunction with the Accounting Division and Program Office. Some of the costs associated with the interface are accounted for within the FHA subsidiary ledger Project. It is likely that Single Family Program Office will need to provide some additional resources.

5.5 Potential Safeguards – Human Capital Risk

As defined in section 4, potential safeguards to reduce human capital risk include:

- Hire contractors to support implementation efforts.

5.5.1 Lifecycle Costs for Acceptable Safeguards

The costs of this safeguard are not included in the estimated lifecycle costs for the project and will likely impose some additional costs on the project.

5.5.2 Effect of Safeguards on Risks

FHA can mitigate human capital risk by implementing safeguards. However, there are still a variety of factors outside of the control of FHA management, such as staff retirement or relocation.

5.5.3 Economic Feasibility of Safeguards

It is critical to the success of the project that FHA monitor potential human resource issues. If FHA cannot provide the project team with the necessary internal resources to staff the project, it is critical to the success of the project to hire knowledgeable contractors to fill the gaps. Detailed costs will be developed as the project progresses.

6.0 RISK REDUCTION RECOMMENDATIONS

6.0 RISK REDUCTION RECOMMENDATIONS

FHA has numerous policies and procedures for protecting its assets against security risks and many other threats. We outline the potential security risks of the proposed system and potential safeguards in Sections 4.2 and 5.2 of this report. In addition, the *System Security and Privacy Plan* outlines the requirements of many federal directives, such as to OMB *Circular A-130 Management of Federal Information Resources*, the *Computer Security Act of 1987*, NIST Special Publications, and the *Privacy Act*. The *System Security and Privacy Plan* also outlines potential measures to address the system requirements and to mitigate the security risks.

APPENDIX A ROLES AND RESPONSIBILITIES

The following table outlines typical roles, responsibilities, and representative work products for the project area team members, including the ASP and any other contractors. FHA will re-evaluate this table with the selected ASP as the project progresses.

Project Team Area	Role	Responsibilities	Representative Work Products
Project Management	▪ Provide leadership, guidance and direction for the Project Team. ▪ Monitor and report project progress to FHA Management and Stakeholders. ▪ Identify and mitigate project risks. ▪ Facilitate communication among project team members from different teams and organizations.	▪ Define scope, objectives, approach and organization. ▪ Define roles and responsibilities. ▪ Define resources. ▪ Establish /maintain work plans. ▪ Define implementation approach.	▪ Updated project plan. ▪ Project scope, objectives, approach. ▪ Project team organization with responsibilities. ▪ Implementation strategy.
QA/Program Office Support	▪ Support the project management team. ▪ Monitor compliance with HUD SDM and other departmental requirements. ▪ Monitor compliance with external entity requirements (i.e., OMB, GAO, etc.). ▪ Prepare documentation for procurements.	▪ Provide quality assurance guidance to project team members. ▪ Prepare status reports. ▪ Record and monitor issues. ▪ Define documentation templates.	▪ Status reports. ▪ Issue tracking reports. ▪ Risk management strategy.

Project Team Area	Role	Responsibilities	Representative Work Products
Functional - Business Process, Documentation	▪ Provide subject matter expertise on current business processes and supporting technical/systems environment. ▪ Define target or "to-be" environment. ▪ Determine process and procedural changes required to align with new property management system.	▪ Confirm current business processes. ▪ Develop "to-be" process. ▪ Define management reports. ▪ Assess gaps between business processes and systems. ▪ Conduct business modeling workshops. ▪ Define and develop standards and procedures. ▪ Develop system documentation. ▪ Work with technical teams to define control tables, configuration, options, interfaces, conversion, and reporting requirements.	▪ Input/output boundary diagram. ▪ High level documentation of current processes, systems. ▪ Conceptual design for target environment. ▪ Gap assessment and recommendations. ▪ Process overview. ▪ Procedures for target environment.

Project Team Area	Role	Responsibilities	Representative Work Products
Stakeholder & End User Communication Management	▪ Design and execute the organizational change and communications needed to support the new property management system. ▪ Support project management team.	▪ Understand stakeholder concerns. ▪ Assess organizational readiness for change. ▪ Align organization with future environment. ▪ Develop communication strategy and plan. ▪ Implement and monitor communications. ▪ Help management prepare the organization for new system and processes.	▪ Communication strategy and plan. ▪ Project web page.
Training	▪ Design and execute the training needed to support the new property management system.	▪ Develop training strategy. ▪ Create/customize end-user training. ▪ Assess skills. ▪ Develop training plan for team and end users. ▪ Develop training documentation. ▪ Deliver end-user training.	▪ Training plan. ▪ Training materials. ▪ Training.
Security Administration	▪ Design and configure the software package to meet FHA’s security requirements.	▪ Conduct risk assessment and define systems risk management procedure. ▪ Design security configuration. ▪ Perform periodic risk assessment. ▪ Define and implement system security plan.	▪ System security plan. ▪ Security configuration design documents. ▪ Risk assessment.

Project Team Area	Role	Responsibilities	Representative Work Products
Conversion and Interfaces	▪ Design and develop conversion and interface programs.	▪ Analyze requirements. ▪ Design programs. ▪ Develop programs.	▪ Interface inventory. ▪ Data conversion strategy. ▪ Design documents. ▪ Conversion and interface programs.
Hardware/Software Infrastructure	▪ Design, implement, and maintain technical infrastructure. ▪ Perform database administration. ▪ Perform operating system administration.	▪ Assess current technical infrastructure. ▪ Design and develop architecture. ▪ Build and test servers, circuits, security components. ▪ Tune technical infrastructure and system. ▪ Conduct performance bench-marking and software configuration. ▪ Prepare an architecture assessment and technical fit analysis reports. ▪ Establish and maintain fit environments.	▪ Target technical architecture workbook.
Application Management	▪ Design and configure the software package to meet FHA requirements.	▪ Analyze fit/gap.	▪ High level fit/gap analysis with alternatives and recommendations.

Project Team Area	Role	Responsibilities	Representative Work Products
Application Administration	▪ Configure system options.	▪ Configure software. ▪ Define application administration processes and procedures. ▪ Configure system administrative features. ▪ Apply patches and fixes.	▪ Configuration design documents.
Reporting	▪ Design and develop reporting programs.	▪ Analyze requirements. ▪ Design reports. ▪ Develop programs.	▪ Design documents. ▪ Reports.
Testing	▪ Design and execute system testing. ▪ Design and execute string testing. ▪ Design and execute integration testing. ▪ Design and execute user acceptance testing.	▪ Develop system test strategy. ▪ Develop system test plan. ▪ Execute system testing.	▪ System test results. ▪ User acceptance test sign-off.